REMARKS

This document is being filed in response to an Office Action mailed 09/05/2005, in which the Examiner said that claims 1-3, 5-41 and 43-53 were pending but rejected. In this amendment, claims 10, 18, 26, and 34 are amended to overcome objections and reasons for rejection given by the Examiner, and other reasons for rejection are traversed below.

Claims to which Objections were Made

In the above-mentioned Office Action, the Examiner said that claims 1 and 34 were objected to because there was a type in claim 1 in "plucality" and in claim 34 in claim 34 in "gtoken." In this amendment, these informalities are corrected.

Claims Rejected under 35 USC §103

Claims Rejected over Baltzley in View of Chandra et al.

In the above-mentioned Office Action, the Examiner said that claims 1-2, 5-14, 16-22, 24-30, 32-38, 40, 43-47 and 49-53 were rejected under 35 USC §103(a) as being unpatentable over U.S. Pat. No. 6,154,153 to Baltzley and further in view of U.S. Pat. No. 4,817,140 to Chandra et al.

Referring to claim 1, in the above-mentioned Office Action, the Examiner said that Baltzley teaches that "said server generates a secure transfer key pair [i.e. as depicted in Figure 3 (see associated descriptions for details)]." The Examiner also said that Baltzley teaches that "said secure transfer key pair is transferred to each of said client computers in said plurality thereof with said private key of said secure transfer key pair in an encrypted form [(i.e. the Enabler computer program communicates with the Server computer program to enable a user to both read encrypted digital messages sent to him or her and send encrypted digital messages to other users. To read encrypted digital messages sent to a user, the user is first prompted by a passphrase. The passphrase is then hashed and

transmitted to the encryption server for authentication. Once the hashed passphrase is authenticated, the encryption server transmits the user's encrypted private key back to the client computer, where it is decrypted. The user may now use the private key to read any digital messages he has received (column 2, lines 38-47)].

Regarding the above statement, the Applicants respectfully submit that the Examiner has described certain end results obtained using the invention of Baltzley, with these results being, to an extent similar to the results obtained using the Applicant's invention, without considering the differences in the processes used to obtain such results, as described in the elements of claim 1. In particular, claim 1 requires that the server must generate a secure transfer key pair and encrypt a private key of the secure transfer pair, and that said secure transfer key pair is transferred to each of said client computers in said plurality thereof with said private key of said secure transfer key pair in an encrypted form. This portion of the process is particularly significant because the secure transfer key pair is shared by all of the client systems that can be operated with a particular token. This is why the secure transfer key pair is transferred to each of the client systems in the plurality thereof, as required by claim 1.

On the other hand, Baltzley does not describe generating a secure transfer key pair and transmitting it to each of the client systems in a group of client systems to be used with a token. Instead, in the system of Baltzley, a new user program is transmitted from the server to the client system, and a key pair is generated in the client system.

Furthermore, Baltzley does not describe the recording of data on computer readable media that are transportable among the client computers. Instead, Baltzley describes the use of a passphrase that is entered by the user, instead of a computer readable medium that is transportable among the client systems.

Chandra et al. describes the use of data recorded on a computer readable medium to enable the operation of a coprocessor, but the client systems, which read the data, are not programmed to generate the data recorded on the computer readable medium. Such data is only generated and recorded in a system manufacturing the media on which the protected information is also being recorded. In particular, Chandra et al. does not describe a secure transfer pair being generated in a server so that token data can subsequently be recorded in a client system separate from the server.

Therefore, the Applicants respectfully submit that Baltzley and Chandra et al., taken separately or in combination, fail to include the requirements of claim 1 for:

said server generates a secure transfer key pair and encrypts a private key of said secure transfer key pair,

said secure transfer key pair is transferred to each of said client computers in said plurality thereof with said private key of said secure transfer key pair in an encrypted form, and

each client computer in said plurality thereof is programmed to generate token data including said portion of said token data encrypted with a public key of said secure transfer key pair, to record said token data on a computer readable medium in said plurality of computer readable media, to read said token data from a computer readable medium in said plurality of computer readable media, to decrypt said private key of said secure transfer key pair, to decrypt said portion of said token data with said private key of said secure transfer key pair, and to be enabled to perform a predetermined task after decrypting said portion of said token data.

For these reasons, the Applicants respectfully submit that claim 1, as amended herein, is patentable under 35 USC §103(a) over Baltzley in view of Chandra et al.

Regarding claims 2 and 9, the Applicants respectfully submit that Baltzley does not teach the requirement of this claim for said secure transfer key pair to be transferred to each of said client computers in said plurality thereof with said private key of said secure transfer key pair encrypted with said public key of said platform key pair of said client computer, and_each client computer in said plurality thereof stores said secure transfer key pair with said private key of said secure transfer key pair encrypted with said public key of said platform key pair and subsequently decrypts said private key of said secure transfer key pair with said private key of said platform key pair. Instead, Baltzley, as shown in FIG. 5, teaches encrypting the private key with a passphrase (step 535), transferring the encrypted private key and plain type public key to an encryption server (step 540), and storing the encrypted private key and plain text public key on the encryption server (step 545). Adding the teachings of Chandra et al. to those of Baltzley does not overcome these deficiencies in describing the limitations of claim 2. Therefore, and additionally because claim 2 merely adds these limitations to claim 1, which is believed to be patentable as described above, the Applicants respectfully submit that claim 2 is patentable under 35 USC §103(a) over Baltzley in view of Chandra et al.

Regarding claims 5-8, these claims were in advertently partially or totally omitted since a single page was inadvertently left out in an earlier amendment. In this amendment, these claims are shown in their original form, since they have not been canceled or amended.

Since these dependent claims merely add limitations to claim 1, the Applicants respectfully submit that these dependent claims are patentable under 35 USC §103(a) over Baltzley in view of Chandra et al. for reasons discussed above regarding claim 1.

Regarding claims 10, 18, and 26, in this amendment, each of these claims is modified to include a requirement that the method enables a computer within a plurality of computers to generate a token causing another computer in the plurality of computer systems to perform a predetermined task. Support for this change is found in the specification as originally filed on page 14, lines 23-25.

Chandra et al. does not describe a method for enabling a computer within a plurality of computers to generate a token causing another computer in the plurality of computers to perform a task. Baltzley does not describe a method for generating a token that is recorded on magnetic media, that is written on a computer readable medium, as required by claims 10, 18, and 26, as amended herein.

Baltzley does not describe the recording of data on computer readable media that are transportable among the client computers. Instead, Baltzley describes the use of a passphrase that is entered by the user, instead of a computer readable medium that is transportable among the client systems. Chandra et al. describes the use of data recorded on a computer readable medium to enable the operation of a coprocessor, but the client systems, which read the data are not programmed to generate the data recorded on the computer readable medium. Such data is only generated and recorded in a system manufacturing the media on which the protected information is also being recorded. In particular, Chandra et al. does not describe a secure transfer pair being generated in a server so that token data can subsequently be recorded in a client system separate from the server.

In the above-mentioned Office Action, the Examiner said, regarding claim 10, that Chandra teaches that software can be distributed on magnetic media (such as tape or floppy disk) or by other means (telephone lines, cable, or broadcast transmission). The software is partitioned into an encrypted portion P_e and an

unencrypted, clear text form P_c. The choice of the partitioning is made by the software vendor with the understanding that only the encrypted portion can be protected from piracy. The encrypted portion, P_e will be protected from piracy. The encrypted portion, P_e of the software will be decrypted and executed by a physically and logically secure coprocessor if the coprocessor possesses the decryption key which embodies the right to execute. The protected part of the softwarte is, thus, never exposed in plaintext form and never executed by unauthorized systems.

Therefore, the Applicants respectfully submit that Baltzley and Chandra et al., taken separately or in combination, fail to include the requirement of claims 10, 18, and 26 for a method to be for generating a token causing a computer system in a plurality of computer systems to be enabled to perform a predetermined task and for reading a token to be enabled to perform a predetermined task, and further for the method to include a step of after storing said secure transfer key pair, in response to an indication that token data is to be recorded, encrypting a portion of said token data with a public key of said secure transfer key pair; and recording said token data, including said portion of said token data encrypted with said public key of said secure transfer key pair on a computer readable medium. The Applicants additionally respectfully submit that Baltzley and Chandra et al. fail to anticipate the requirement of claims 10, 18, and 26 for the secure token to be transmitted from a server separate from the computer system subsequently using it to write and read the token data. For these reasons, the Applicants respectfully submit that claims 10, 18, and 26, as amended herein, are patentable under 35 USC §103(a) over Baltzley in view of Chandra et al.

Regarding claims 11-14, 16 and 17, since these dependent claims merely add limitations to claim 10, the Applicants respectfully submit that these dependent claims are patentable under 35 USC §103(a) over Baltzley in view of Chandra et al. for reasons discussed above regarding claims 10, 18, and 26.

Regarding claims 19-22, 24 and 25, since these dependent claims merely add limitations to claim 18, the Applicants respectfully submit that these dependent claims are patentable under 35 USC §103(a) over Baltzley in view of Chandra et al. for reasons discussed above regarding claims 10, 18, and 26.

Regarding claims 27-30, 32 and 33, since these dependent claims merely add limitations to claim 26, the Applicants respectfully submit that these dependent claims are patentable under 35 USC §103(a) over Baltzley in view of Chandra et al. for reasons discussed above regarding claims 10, 18, and 26.

Regarding claim 34, in the above-mentioned Office Action, the Examiner said that Baltzley teaches generating a secure transfer key pair within a server, with the New User computer program communicating with the Server computer program to generate a public/private key pair, a user identifier, and a user passphrase. The Examiner further said that, once the hashed passphrase is authenticated, the encryption server transmits the user's encrypted private key back to the client computer, where it is decrypted, so that the user may use the private key to read any digital messages he has received. The Examiner referred to column 2, lines 44-48 and FIG. 6, and further said that it is further understood that a client machine or computer or device is also a client/server.

Regarding the above statement, the Applicants note that claim 34 includes requirements that the secure transfer key pair must be generated in a server that is separate from the local computer and the remote computer (which are both client computers). On the other hand, Baltzley teaches, as shown in FIG. 5, and as described in reference thereto, that the New User computer program is downloaded from the encryption server to the client system in step 510 and that the public/private key pair is then generated within the client computer in step 520. The fact that certain operations occur within the local (client) computer

while other operations occur within the server is significant in the Applicants' invention, since the physical structures of these systems can provide certain types of security.

The Examiner additionally said that Baltzley teaches the requirement of claim 34 for transferring said secure transfer key pair from said server to said remote computer and for storing said secure transfer key pair within said remote computer.

Regarding this statement, the Applicants note that a key feature of their invention lies in the fact that a secure transfer key pair is generated within the server, and that this secure transfer key pair is transmitted from the server to both the local computer and the remote computer. This is the method that is used to identify all of the remote computers that can be used with a particular token generated in accordance with the invention. The Applicants respectfully submit that Baltzley does not teach or describe the generation of a secure transfer key pair that is then transmitted to both a local computer and a remote computer.

The Applicants further submit that Chandra et al. teaches against transferring a secure transfer key pair from a server to a local computer and to a remote computer, teaching instead, on column 4, lines 18-36, that a number of keys should be placed within the computer systems at the time of their manufacture. Therefore, adding the teachings of Chandra et al. to those of Baltzley does not overcome the deficiencies of Baltzley in terms of describing requirements for generating a secure transfer key pair within a server and transmitting the secure transfer key pair to a local computer and to a remote computer.

For the above reasons, the Applicants respectfully submit that Baltzley and Chandra et al, taken separately or in combination, do not teach, describe, or otherwise anticipate the requirements of claim 34 for:

generating a secure transfer key pair within a server separate from said local computer and from said remote computer;

transferring said secure transfer key pair from said server to said local computer;

storing said secure transfer key pair within said local computer;

establishing communication between said remote computer and said server;

transferring said secure transfer key pair from said server to said remote computer;

storing said secure transfer key pair within said remote computer;

Therefore, the Applicants respectfully submit that claim 34, as amended herein, is patentable under 35 USC §103(a) over Baltzley in view of Chandra et al.

Regarding claims 35-38, 40, and 43, since these dependent claims merely add limitations to claim 34, the Applicants respectfully submit that these dependent claims are patentable under 35 USC §103(a) over Baltzley in view of Chandra et al. for reasons discussed above regarding claims 10, 18, and 34.

Regarding claims 44 and 50, the Applicants note that Baltzley does not describe the recording of data on computer readable media that are transportable among the client computers. Instead, Baltzley describes the use of a passphrase that is entered by the user, instead of a computer readable medium that is transportable among the client systems. Chandra et al. describes the use of data recorded on a computer readable medium to enable the operation of a coprocessor, but the client systems, which read the data are not programmed to generate the data recorded on the computer readable medium. Such data is only generated and recorded only in a system manufacturing the media on which the protected information is also being recorded. In particular, Chandra et al. does not describe a secure transfer pair being generated in a

server so that token data can subsequently be recorded in a client system separate from the server.

Applicants note that claims 44 and 50 include requirements that the secure transfer key pair must be generated in a server that is separate from the plurality of computer systems. On the other hand, Baltzley teaches, as shown in FIG. 5, and as described in reference thereto, that the New User computer program is downloaded from the encryption server to the client system in step 510 and that the public/private key pair is then generated within the client computer in step 520. The fact that certain operations occur within the local (client) computer while other operations occur within the server is significant in the Applicants' invention, since the physical structures of these systems can provide certain types of security.

The Applicants further note that a key feature of their invention lies in the fact that a secure transfer key pair is generated within the server, and that this secure transfer key pair is transmitted from the server to each client computer in the plurality of client computers. This is the method that is used to identify all of the client computers that can be used with a particular token generated in accordance with the invention. The Applicants respectfully submit that Baltzley does not teach or describe the generation of a secure transfer key pair that is then transmitted to a plurality of associated client computers..

The Applicants further submit that Chandra et al. teaches against transferring a secure transfer key pair from a server to a local computer and to a remote computer, teaching instead, on column 4, lines 18-36, that a number of keys should be placed within the computer systems at the time of their manufacture. Therefore, adding the teachings of Chandra et al. to those of Baltzley does not overcome the deficiencies of Baltzley in terms of describing requirements for

generating a secure transfer key pair within a server and transmitting the secure transfer key pair to a a plurality of associated client computers..

Therefore, the Applicants respectfully submit that Baltzley and Chandra et al., taken separately or in combination, fail to include the requirement of claims 44 and 50, as modified herein, for the generation of a secure transfer key pair in a server separate from the plurality of associated client servers and for the transfer of the secure transfer key from the server to each client computer within the plurality of client computers. For this reason, the Applicants respectfully submit that claims 44 and 50 are patentable under 35 USC §103(a) over Baltzley in view of Chandra et al.

Regarding claims 45-47 and 49, since these dependent claims merely add limitations to claim 44, the Applicants respectfully submit that these dependent claims are patentable under 35 USC §103(a) over Baltzley in view of Chandra et al. for reasons discussed above regarding claims 44 and 50

Regarding claims 51-53, since these dependent claims merely add limitations to claim 50, the Applicants respectfully submit that these dependent claims are patentable under 35 USC §103(a) over Baltzley in view of Chandra et al. for reasons discussed above regarding claims 44 and 50.

Claims Rejected over Baltzley in View of Taaffe

In the above-mentioned Office Action, the Examiner said that claims 3, 15, 23, 31, 39, 41, and 48 were rejected under 35 USC §103(a) as being unpatentable over U.S. Pat. No. 6,154,153 to Baltzley and further in view of U.S. Pat. No. 4,747,139 to Taffee.

Regarding claim 3, the Applicants respectfully submit that adding the disclosure of Taffee to that of Baltzley does not overcome the deficiencies of Baltzley in describing the limitations of claim 1, to which claim 3 merely adds limitations, with these deficiencies having been described in detail above regarding claim 1, and that, therefore, claim 3 is patentable under 35 USC §103(a) over Baltzley in view of Taffee.

Regarding claim 15, the Applicants respectfully submit that adding the disclosure of Taffee to that of Baltzley does not overcome the deficiencies of Baltzley in describing the limitations of claim 10, to which claim 15 merely adds limitations, with these deficiencies having been described in detail above regarding claim 10, and that, therefore, claim 15 is patentable under 35 USC §103(a) over Baltzley in view of Taffee.

Regarding claim 23, the Applicants respectfully submit that adding the disclosure of Taffee to that of Baltzley does not overcome the deficiencies of Baltzley in describing the limitations of claim 18, to which claim 23 merely adds limitations, with these deficiencies having been described in detail above regarding claim 18, and that, therefore, claim 23 is patentable under 35 USC §103(a) over Baltzley in view of Taffee.

Regarding claim 31, the Applicants respectfully submit that adding the disclosure of Taffee to that of Baltzley does not overcome the deficiencies of Baltzley in describing the limitations of claim 26, to which claim 31 merely adds limitations, with these deficiencies having been described in detail above regarding claim 26, and that, therefore, claim 31 is patentable under 35 USC §103(a) over Baltzley in view of Taffee.

Regarding claims 39 and 41, the Applicants respectfully submit that adding the disclosure of Taffee to that of Baltzley does not overcome the deficiencies of

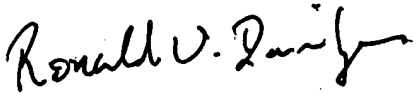
Baltzley in describing the limitations of claim 34, to which claims 39 and 41 merely add limitations, with these deficiencies having been described in detail above regarding claim 34, and that, therefore, claims 39 and 41 are patentable under 35 USC §103(a) over Baltzley in view of Taffee.

Regarding claim 48, the Applicants respectfully submit that adding the disclosure of Taffee to that of Baltzley does not overcome the deficiencies of Baltzley in describing the limitations of claim 44, to which claim 48 merely adds limitations, with these deficiencies having been described in detail above regarding claim 44, and that, therefore, claim 48 is patentable under 35 USC §103(a) over Baltzley in view of Taffee.

Conclusions

The Applicants respectfully submit that the application, including claims 1-3, 5-41, and 43-53 is now in condition for allowance, and that action is earnestly requested, with reconsideration and reversal of reasons given for rejections.

Respectfully Submitted,



Ronald V. Davidge
Registration No. 33,863
Telephone No. 954-344-9880
January 2, 2006